PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-066879
(43)Date of publication of application : 03.03.2000

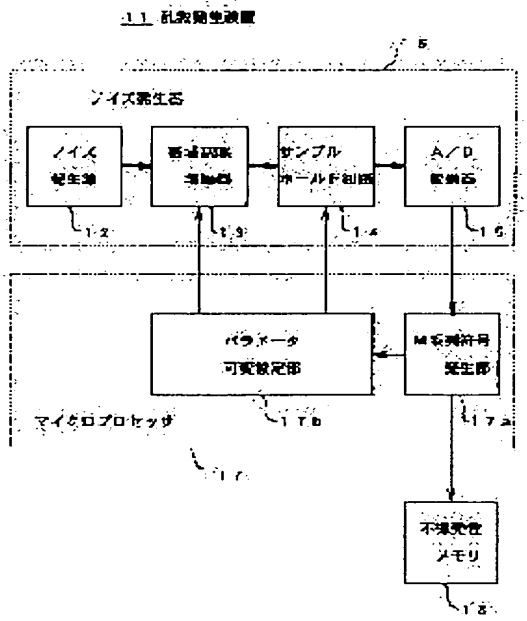
(51)Int.Cl. G06F 7/58

(21)Application number : 10-235175
(22)Date of filing : 21.08.1998

(71)Applicant : NEC CORP
(72)Inventor : SATO YUZURU

(54) RANDOM NUMBER GENERATOR

(57)Abstract:
PROBLEM TO BE SOLVED: To generate the random number of high randomness by compounding software processing and a hardware.
SOLUTION: A noise generated by a noise generating source 12 is amplified while limiting the band through a band limit amplifier 13, further, sampled by a sample/hold circuit 14 and converted to a digital signal stream and a random number is generated by performing software processing to the provided signal stream through an M system code generating part 17a in a microprocessor 17. The trouble of simultaneously generating the same random number at two different spots is avoided and as the random number, reliability can be surely improved.



(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－66879
（P2000－66879A）
(43)公開日　平成12年３月３日(2000.3.3)

(51)Int.Cl.⁷	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　7/58		Ｇ０６Ｆ　7/58	Ｃ

審査請求　未請求　請求項の数６　ＯＬ　（全　５　頁）

(21)出願番号　特願平10－235175

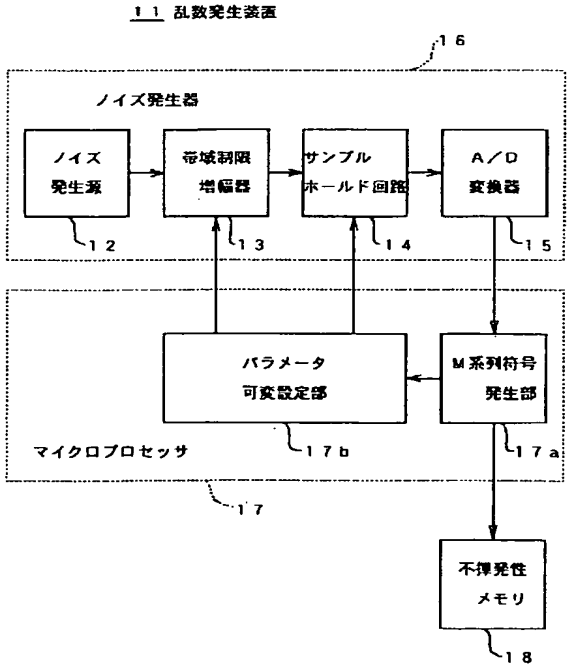
(22)出願日　平成10年８月21日(1998.8.21)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　佐藤　譲
大阪府大阪市中央区城見一丁目４番24号
日本電気ホームエレクトロニクス株式会社
内
(74)代理人　100108578
弁理士　高橋　詔男　（外３名）

(54)【発明の名称】　乱数発生装置

(57)【要約】
【課題】　ソフトウェア処理とハードウェアとを複合してランダム性の高い乱数を発生させる。
【解決手段】　ノイズ発生源１２が発生するノイズを、帯域制限増幅器１３により帯域制限して増幅し、さらにこれをサンプルホールド回路１４において標本化してディジタル信号列に変換し、得られた信号列をマイクロプロセッサ１７内のM系列符号発生部１７ａにおいてソフトウェア処理して乱数を発生する。同じ乱数が異なる二箇所で同時に発生する不都合を排除し、乱数としての信頼性を確実に高めることができる。

本発明の乱数発生装置の一実施形態を示す概略ブロック構成図



1

【特許請求の範囲】

【請求項１】　ノイズを発生するノイズ発生源と、該ノイズ発生源から供給されるノイズを帯域制限して増幅する帯域制限増幅器と、該帯域制限増幅器の出力を標本化するサンプルホールド回路と、該サンプルホールド回路の標本化出力をディジタル信号列に変換するＡ／Ｄ変換器と、該Ａ／Ｄ変換器の出力をソフトウェア処理して乱数を発生するマイクロプロセッサとを具備することを特徴とする乱数発生装置。

【請求項２】　前記ノイズ発生源は、熱雑音や或いは白色雑音に相当する周期性のないノイズを発生することを特徴とする請求項１記載の乱数発生装置。

【請求項３】　前記マイクロプロセッサは、前記ＡＤ変換器の出力を初期値としてソフトウェア処理によりＭ系列符号を発生することを特徴とする請求項１記載の乱数発生装置。

【請求項４】　ノイズを発生するノイズ発生源と、通過帯域及び増幅度が外部から可変設定され、前記ノイズ発生源から供給されるノイズを帯域制限して増幅する帯域制限増幅器と、標本化タイミングを外部から可変設定され、前記帯域制限増幅器の出力を標本化するサンプルホールド回路と、該サンプルホールド回路の標本化出力をディジタル信号列に変換するＡ／Ｄ変換器と、該Ａ／Ｄ変換器の出力をソフトウェア処理して乱数を発生するとともに、該乱数に基づいて前記帯域制限増幅器の通過帯域及び増幅度か又は前記サンプルホールド回路の前記標本化タイミングの少なくとも一方を可変設定するマイクロプロセッサとを具備することを特徴とする乱数発生装置。

【請求項５】　前記ノイズ発生源は、熱雑音や或いは白色雑音に相当する周期性のないノイズを発生することを特徴とする請求項４記載の乱数発生装置。

【請求項６】　前記マイクロプロセッサは、前記ＡＤ変換器の出力を初期値としてソフトウェア処理によりＭ系列符号を発生することを特徴とする請求項４記載の乱数発生装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ソフトウェア処理とハードウェアとを複合してランダム性の高い乱数を発生させるようにした乱数発生装置に関する。

【０００２】

【従来の技術】高速道路の料金所において利用料金を自動的に徴収する自動料金収受システム（ＥＴＣ）の導入を控え、路車間通信に必要な通信装置を搭載した車両の開発が進められている。高速道路自動料金収受システムを利用する車両は、料金所の手前の所定の通信エリア内に達した段階で、路側ビーコンを介して料金所と通信接続確立を行う必要があり、初期接続処理用として例えば３２ビットのリンクＩＤを用いて通信接続確立を行う方法が検討されている。ただし、同一の路側ビーコン通信エリア内では他の車載通信装置との通信上の衝突を避ける必要があり、このためリンクＩＤに非常に高いランダム性を与える乱数発生装置を開発する必要がある。

2

【０００３】図２に示す従来の乱数発生装置１は、乱数発生ソフトウェアを搭載したマイクロプロセッサ２が、初期接続処理用として３２ビットのリンクＩＤを発生するものであり、ここでは乱数としてＭ系列符号を用いるようにしている。マイクロプロセッサ２は、ソフトウェア処理によりＭ系列符号を発生するのであるが、符号発生原理を説明しやすいよう、ここでは便宜的にハードウェア構成になぞらえてマイクロプロセッサ２の内部ブロックを図示してある。

【０００４】ソフトウェアが実現するＭ系列符号発生手段は、０又は１の状態を記憶する１ビットのレジスタ３ａを３２段に亙って縦列接続したシフトレジスタ３と、特定段のレジスタ３ａからデータを取り出して帰還させる帰還タップ４と、帰還タップ４からの出力を加算して初段のレジスタ３ａに帰還する加算器（排他的論理和回路）５とから構成され、各レジスタ３ａが保持するビットデータは所定の動作クロックに従って順次シフトされる。なお、帰還タップ４の位置は特定段に設定する必要があり、こうすることで、所定周期で所定の変化形態を示すＭ系列符号を発生することができる。また、初期状態として３２段のシフトレジスタ３の全てのレジスタ３ａに「０」がセットされるオール０の状態を避けるため、Ｍ系列符号発生開始時に初期値として例えばオール１等のデータをセットするよう、初期値を保持する初期値レジスタ６がシフトレジスタ３に併設してあり、車両が路側ビーコンとの通信エリア内に進入したときに作動する起動トリガ回路７から供給されるトリガ信号により、初期値レジスタ６の保持データが初期値としてシフトレジスタ３に移送されるようになっている。

【０００５】

【発明が解決しようとする課題】上記従来の乱数発生装置１が発生する乱数の精度は、マイクロプロセッサ２に搭載した乱数発生ソフトウェアに依存するのは当然であるが、Ｍ系列符号の初期値は乱数発生ソフトウェアの起動タイミングをもってセットされる。このため、起動タイミングが偶然重なってしまった２台の車両については、同じ初期値を用いてＭ系列符号を発生する結果、同じ乱数をリンクＩＤとして用いてしまうことがあり、通信障害を招く恐れがあった。これは、乱数発生ソフトウェアの起動タイミングが幅広く分散していないことにも一因があるが、いずれにしてもＭ系列符号として得られる乱数のランダム性が乏しくなるほど、他の車載通信装置との通信上の衝突を招く危険が増え、料金収受システム自体の円滑な運用の妨げとなるため、乱数のランダム性を高める対策を講じなければならないといった課題があった。

【０００６】本発明は、上記課題を解決したものであり、乱数発生ソフトウェアが必要とする初期値をノイズ発生用のハードウェアから供給し、ランダム性の高い乱数を発生することを目的とするものである。

【０００７】

【課題を解決するための手段】上記目的を達成するため、本発明は、ノイズを発生するノイズ発生源と、該ノイズ発生源から供給されるノイズを帯域制限して増幅する帯域制限増幅器と、該帯域制限増幅器の出力を標本化するサンプルホールド回路と、該サンプルホールド回路の標本化出力をディジタル信号列に変換するＡ／Ｄ変換器と、該Ａ／Ｄ変換器の出力をソフトウェア処理して乱数を発生するマイクロプロセッサとを具備することを特徴とするものである。

【０００８】また、本発明は、ノイズを発生するノイズ発生源と、通過帯域及び増幅度が外部から可変設定され、前記ノイズ発生源から供給されるノイズを帯域制限して増幅する帯域制限増幅器と、標本化タイミングを外部から可変設定され、前記帯域制限増幅器の出力を標本化するサンプルホールド回路と、該サンプルホールド回路の標本化出力をディジタル信号列に変換するＡ／Ｄ変換器と、該Ａ／Ｄ変換器の出力をソフトウェア処理して乱数を発生するとともに、該乱数に基づいて前記帯域制限増幅器の通過帯域及び増幅度か又は前記サンプルホールド回路の前記標本化タイミングの少なくとも一方を可変設定するマイクロプロセッサとを具備することを特徴とするものである。

【０００９】

【発明の実施の形態】以下、本発明の実施形態を図１を参照して説明する。図１は、本発明の乱数発生装置の一実施形態を示す概略ブロック構成図である。

【００１０】図１に示す乱数発生装置１１は、ノイズ発生源１２と帯域制限増幅器１３とサンプルホールド回路１４とＡ／Ｄ変換器１５とを縦列接続して構成したノイズ発生器１６と、乱数発生ソフトウェアを搭載したマイクロプロセッサ１７と、マイクロプロセッサ１７が発生した乱数を書き込む不揮発性メモリ１８等から構成される。マイクロプロセッサ１７は、機能的に分割集約して図示した２ブロックからなり、乱数発生ソフトウェアに従って動作するM系列符号発生部１７ａと、発生した乱数に応じてパラメータを可変設定するパラメータ可変設定部１７ｂがこれらのブロックに該当する。

【００１１】ノイズ発生源１２は、熱雑音や或いは白色雑音に相当する周期性のないノイズを発生する働きをするものであり、本実施形態では、例えば抵抗器の両端に発生する熱雑音を増幅してコンパレータにおいてしきい値判別することによりノイズを発生させる構成が用いられる。帯域制限増幅器１３は、通過帯域及び増幅度がマイクロプロセッサ１７内のパラメータ可変設定部１７ｂにより可変設定され、ノイズ発生源１２から供給されるノイズを帯域制限して増幅する。サンプルホールド回路１４は、標本化タイミングをマイクロプロセッサ１７内のパラメータ可変設定部１７ｂにより可変設定され、帯域制限増幅器１３の出力を標本化する。Ａ／Ｄ変換器１５は、サンプルホールド回路１４の標本化出力を量子化してディジタル信号列に変換し、マイクロプロセッサ１７内のM系列符号発生部１７ａに初期値として与える。

【００１２】ここで、ノイズ発生源１２は、周期性も再現性ももたない熱雑音を発生し、これを帯域制限増幅器１３を介してサンプルホールド回路１４に供給する。帯域制限増幅器１３の通過帯域幅と増幅度は、マイクロプロセッサ１７内のパラメータ可変設定部１７ｂが出力する通過帯域幅と増幅度を指定するパラメータにより設定されており、同様にサンプルホールド回路の標本化タイミングもまた、マイクロプロセッサ１７内のパラメータ可変設定部１７ｂが出力する標本化タイミングを指定するパラメータにより設定されている。従って、ノイズ発生源１２が発生したノイズは、前回生成した乱数に応じて設定されたパラメータに従って帯域制限されかつ増幅され、続いて標本化される。

【００１３】サンプルホールド回路５によって標本化されたノイズは、Ａ／Ｄ変換器１５に供給され、ここで量子化されてディジタル数値列に変換される。ディジタル数値列は、マイクロプロセッサ１７内のM系列符号発生部１７ａに初期値として供給される。M系列符号発生部１７ａは、Ａ／Ｄ変換器１５から供給されたディジタル数値列を初期値としてM系列符号を発生するが、ここで発生したM系列符号は乱数として不揮発性メモリ１８に格納保存され、これが高速道路料金収受システムのための接続確認用リンクＩＤとして用いられる。また、この乱数はパラメータ可変設定部１７ｂに供給され、次回のリンクＩＤ作成時にノイズ発生器１６内で必要になる通過帯域幅及び増幅度と標本化タイミングの設定に供される。

【００１４】このように、上記乱数発生装置１１によれば、ノイズ発生源１２が発生するノイズを帯域制限して増幅し、さらにこれを標本化してディジタル信号列に変換し、得られた信号列をソフトウェア処理して乱数を発生する構成としたから、与えられた初期値に基づいて単純にソフトウェア処理によりて乱数を発生する従来装置１のように、初期値を与えるタイミングが偶然に重なってしまった場合に、同じ乱数が異なる二箇所で同時に発生するといったランダム性を損なう問題が発生することは殆どない。また、ノイズ発生源１２がハードウェアに固有のランダム性をもって発生する規則性をもたないノイズにより、ソフトウェア処理に供するディジタル信号列を真のランダム性をもって発生することができ、同じ乱数が異なる二箇所で同時に発生する不都合を徹底的に排除し、発生乱数の信頼性を確実に高めることができる。

【００１５】また、仮にノイズ発生源１２自体のノイズ発生に関する非周期性が外乱による影響を受けたとしても、ノイズに由来する数値に基づいて乱数を発生するマイクロプロセッサ１７が、この乱数に基づいてパラメータ（通過帯域幅及び増幅度と標本化タイミング）を可変設定するため、この帰還的修正とハードウェア処理との相乗効果により、きわめて高いランダム性をもって乱数を発生させることができる。

【００１６】また、ノイズ発生源１２が、熱雑音や或いは白色雑音に相当する周期性のないノイズを発生する構成としたから、例えば抵抗器の熱雑音をコンパレータにてしきい値判別するといったハードウェア処理により安定したノイズの発生が可能であり、電気的或いは機械的に発生した周期性や再現性をもたないノイズを用い、マイクロプロセッサ１７によるソフトウェア処理による乱数発生を確実なものとすることができる。また、マイクロプロセッサ１７が、Ａ／Ｄ変換器１５の出力を初期値としてソフトウェア処理によりＭ系列符号を発生するため、Ａ／Ｄ変換器１５を介して与えられるノイズをもってＭ系列符号の初期値を設定することで、Ｍ系列符号がもつランダム性を有効活用することができ、同じ乱数が異なる二箇所で同時に発生する不都合を良好に排除することができる。

【００１７】なお、上記実施形態において、マイクロプロセッサ１７が発生した乱数に応じて帯域制限増幅器１３の通過帯域及び増幅度とサンプルホールド回路１４の標本化タイミングの両方を可変設定する構成としたが、帯域制限増幅器１３の通過帯域及び増幅度とサンプルホールド回路１４の標本化タイミングのいずれか一方だけをマイクロプロセッサ１７が発生した乱数に応じて可変設定するようにしてもよい。また、マイクロプロセッサ１７内のパラメータ可変設定部１７ｂは省略することもでき、その場合は、帯域制限増幅器１３の通過帯域及び増幅度も或いは帯域制限増幅器１３に接続されるサンプルホールド回路１４の標本化タイミングも固定されることになるが、ノイズ発生源１２のランダム性に依存する乱数発生は可能である。

【００１８】

【発明の効果】以上に説明したように、本発明によれば、ノイズ発生源が発生するノイズを帯域制限して増幅し、さらにこれを標本化してディジタル信号列に変換し、得られた信号列をソフトウェア処理して乱数を発生する構成としたから、与えられた初期値に基づいて単純にソフトウェア処理により乱数を発生する従来装置のように、初期値を与えるタイミングが偶然に重なってしまった場合に、同じ乱数が異なる二箇所で同時に発生するといったランダム性を損なう問題が発生することは殆どなく、ノイズ発生源がハードウェアに固有のランダム性をもって発生する規則性をもたないノイズにより、ソフトウェア処理に供するディジタル信号列を真のランダム性をもって発生することができ、同じ乱数が異なる二箇所で同時に発生する不都合を徹底的に排除し、発生乱数の信頼性を確実に高めることができる等の優れた効果を奏する。

【００１９】また、本発明は、ノイズ発生源に接続される帯域制限増幅器の通過帯域及び増幅度か又は帯域制限増幅器に接続されるサンプルホールド回路の標本化タイミングの少なくとも一方を、マイクロプロセッサが発生乱数に従って可変設定する構成としたから、仮にノイズ発生源自体のノイズ発生に関する非周期性が外乱による影響を受けたとしても、ノイズに由来する数値に基づいて乱数を発生するマイクロプロセッサが、この乱数に基づいて通過帯域幅及び増幅度と標本化タイミングを可変設定するため、この帰還的修正とハードウェア処理との相乗効果により、きわめて高いランダム性をもって乱数を発生させることができる等の効果を奏する。

【００２０】また、ノイズ発生源が、熱雑音や或いは白色雑音に相当する周期性のないノイズを発生する構成としたから、例えば抵抗器の熱雑音をコンパレータにてしきい値判別するといったハードウェア処理により安定したノイズの発生が可能であり、電気的或いは機械的に発生した周期性や再現性をもたないノイズを用い、マイクロプロセッサによるソフトウェア処理による乱数発生を確実なものとすることができる等の効果を奏する。

【００２１】また、マイクロプロセッサが、Ａ／Ｄ変換器の出力を初期値としてソフトウェア処理によりＭ系列符号を発生するため、Ａ／Ｄ変換器を介して与えられるノイズをもってＭ系列符号の初期値を設定することで、Ｍ系列符号がもつランダム性を有効活用することができ、同じ乱数が異なる二箇所で同時に発生する不都合を良好に排除することができる等の効果を奏する。

【図面の簡単な説明】

【図１】本発明の乱数発生装置の一実施形態を示す概略ブロック構成図である。

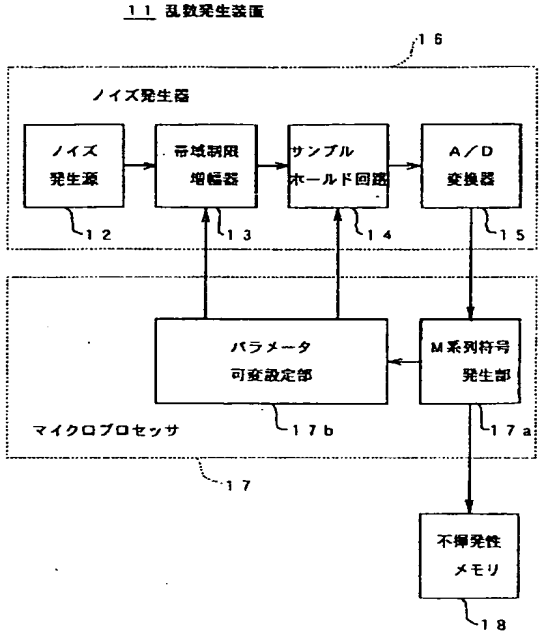
【図２】従来の乱数発生装置の一例を示す概略ブロック構成図である。

【符号の説明】

１１　乱数発生装置
１２　ノイズ発生源
１３　帯域制限増幅器
１４　サンプルホールド回路
１５　Ａ／Ｄ変換器
１６　ノイズ発生器
１７　マイクロプロセッサ
１７ａ　Ｍ系列符号発生部
１７ｂ　パラメータ可変設定部
１８　不揮発性メモリ

【図１】

本発明の乱数発生装置の一実施形態を示す概略ブロック構成図



【図２】

従来の乱数発生装置の一例を示す概略ブロック構成図